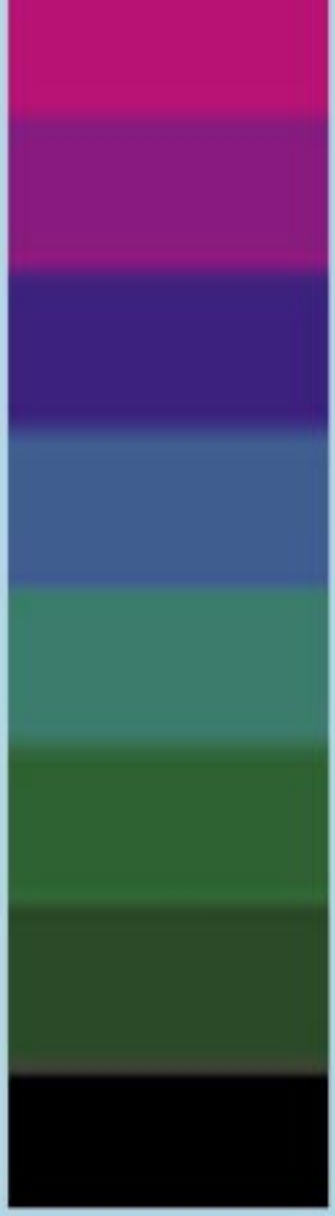
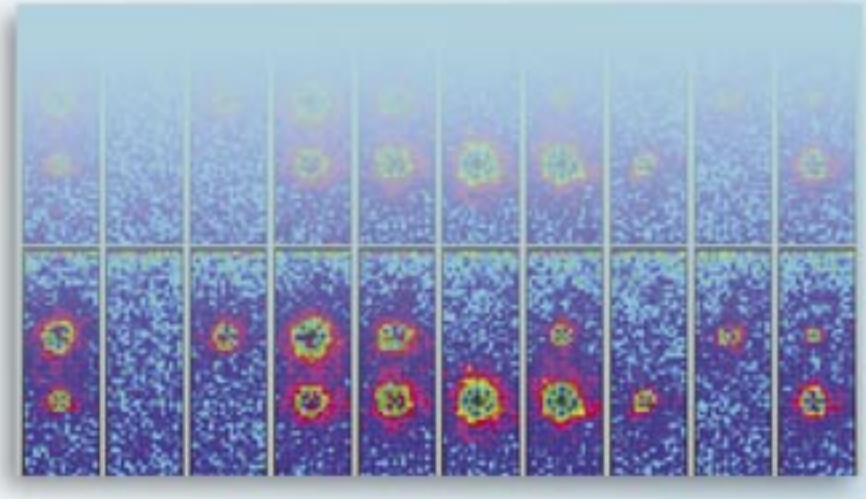
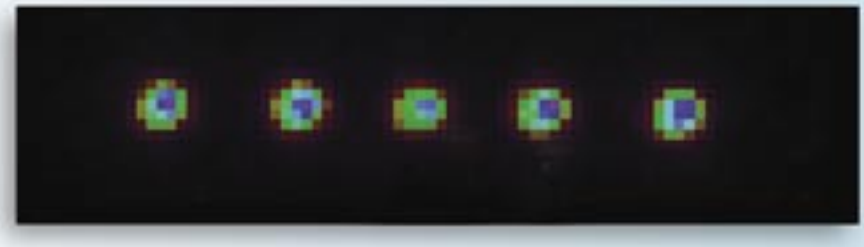
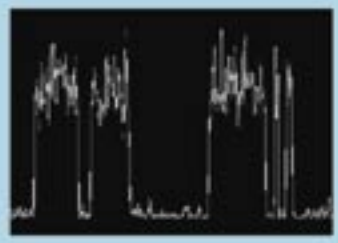
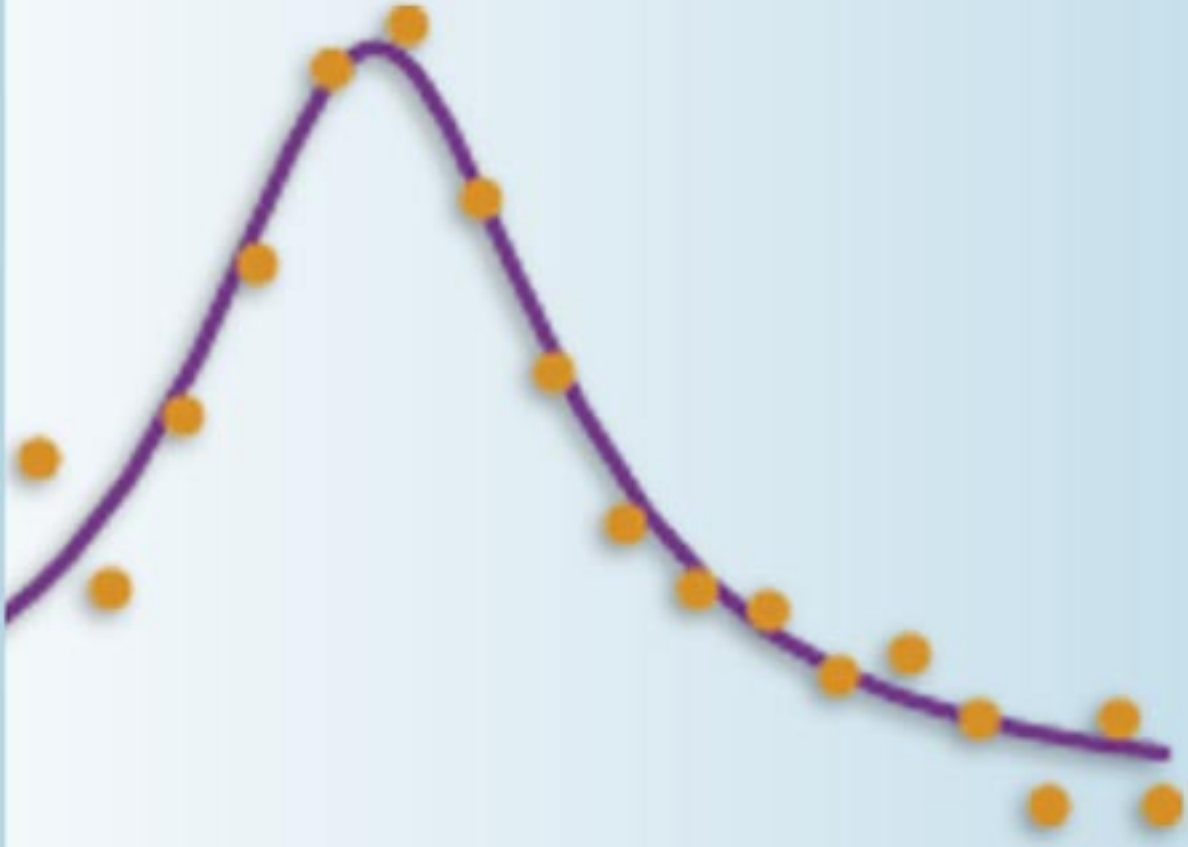
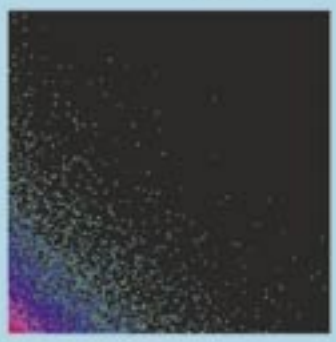




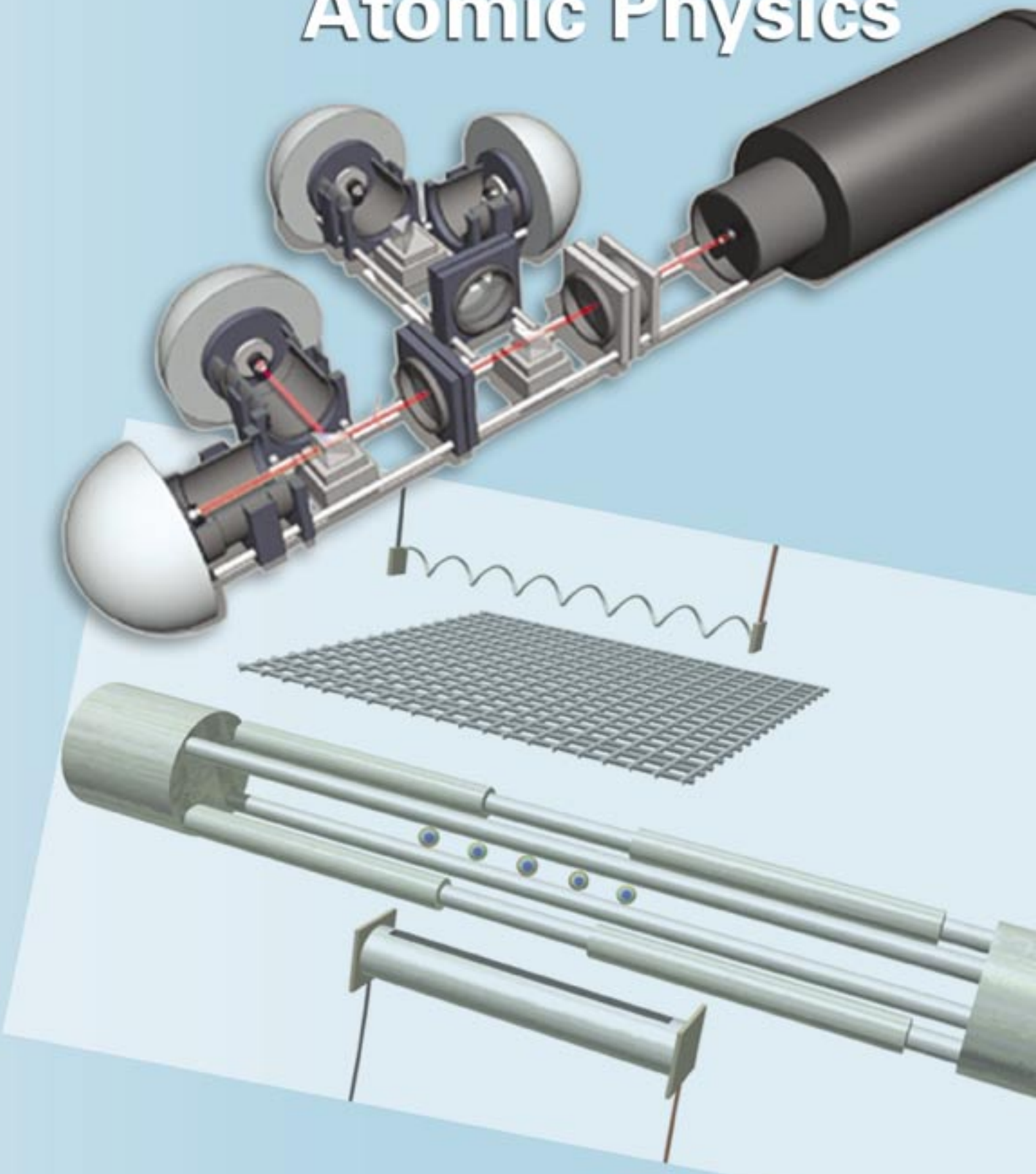








Atomic Physics



Atomic Physics Contents

Research Highlights

Testing the Randomness of Quantum Mechanics

D.J. Berkeland (P-21)

Possibly the most nonintuitive aspect of quantum mechanics is that a single particle can be put into a superposition of two distinct states. Moreover, when one makes a measurement, the particle is found in only one state, and that result is unpredictable, or random. Since its inception, quantum theory has been rigorously tested under many diverse conditions and often with extremely high precision. Surprisingly, there are very few statistically significant tests of the *randomness* of a quantum-mechanical process, including the transitions between quantum states. Some experiments have monitored the decays of a large sample of nuclear particles, whereas others have measured whether a photon is transmitted or reflected from a beamsplitter. However, these methods have limitations such as accounting for interactions between their nuclei or the inability to detect every decay particle or photon—only a small level of paranoia is required to imagine that the detectors are missing patterns in the directions of decaying particles or in the timing of photon transmissions.

It is important to improve these tests of the statistics of quantum-mechanical processes for several reasons. First, quantum mechanics is such a fundamental part of our view of the physical world that we must test it as carefully as possible. History is full of scientific theories that were widely accepted until precise and accurate measurements illuminated their subtle deficiencies. Second, applications such as quantum cryptography rely on the generation of strings of numbers that are as random as possible. Devices based on quantum-mechanical processes are ideal candidates for quantum cryptography. We must therefore demonstrate that the underlying processes behind these devices are indeed free of cyclic behavior and correlations between number sequences. Finally, the trapped strontium ions that we use to perform our experiments could also be used to implement a quantum computer. It is imperative that the quantum-mechanical processes that make quantum computation so powerful are not compromised by systematic effects. For all these reasons, we have developed an experimental system based on trapped strontium ions that permits us to observe spontaneous and laser-induced transitions between internal states in single ions and pairs of ions. We then statistically analyze them, searching for signs of memory in these physical systems and patterns in their behavior.

Trapping Ions to Study Quantum Effects

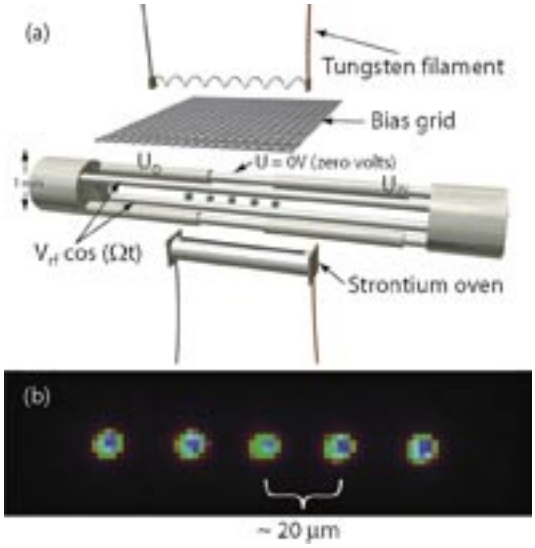
Our tests of quantum mechanics are, in principle, cleaner than those of previous experiments because we monitor the transitions of a single ion between two sets of its internal states. Because we use only a single ion that is suspended in space and localized to less then 100 nm by electric fields, our experiments are not susceptible to multiparticle effects. Also, because we can tell with near-unity efficiency the state of the ion, our experiments are immune to detector-efficiency loopholes. Previous researchers have used a similar trapped-ion system to analyze approximately 1,000 such transitions; we analyze

Figure 1. A time series of two ions simultaneously undergoing quantum jumps.

240,000 transitions in single ions and 230,000 transitions and 8,600 spontaneous decays in two simultaneously trapped ions.

To do this, we first confine ions in a trap such as that shown in Figure 2(a).[1] An rf voltage is applied to two diagonally opposite rods, while dc potentials are applied to the remaining electrodes. This creates a time-averaged potential that forces ions towards the trap's long axis. We apply several hundred volts to the "sleeve" electrodes to keep the ions from leaking from the ends of the trap. Ions are formed inside the trap when neutral strontium vapor from a small oven intersects with an electron beam from a tungsten filament. The whole apparatus is inside a small chamber at ultra-high-vacuum conditions.

Typically, tens of ions are created inside the trap. They make a relatively hot cloud that is hundreds of microns long and about a hundred microns in diameter. The motion of the ions is forced by the trap's rf electric field and by the Coulomb interactions between the charged ions, and individual ions cannot be distinguished. In this state, they are not useful for our experiments, so we reduce their motion by Doppler cooling them with laser light. In this process, 422-nm laser light is tuned slightly below the ions' $S_{1/2} \leftrightarrow P_{1/2}$ resonance (Figure 3). When ions travel towards the light source, they absorb a 422-nm photon, which reduces their speed due to conservation of momentum. On the other hand, if the ion is moving away from the light source and absorbs a photon, its speed increases. But the frequency of the laser light is such that an ion moving away from the light source is Doppler shifted far out of resonance with the light. So, on average, the laser light cools the ions.



When the ions are cold enough, they undergo a sudden phase change, freezing into ion crystals such as that shown in Figure 2(b). This shows a crystal of five strontium ions that scattered 422-nm light into an imaging camera. The ions are forced together by the trap potential that we have applied to the sleeve electrodes, and they are forced apart because they are all positively charged. Typically, the ions are spaced tens of microns apart. We have formed linear chains of approximately 40 ions but typically experiment with only a single ion in the trap. Once an ion is trapped and laser cooled, it stays in the trap indefinitely so that we can perform experiments that were considered impossible when quantum mechanics was first conceived.

Observing Quantum Jumps in Trapped Ions

For example, we can observe quantum jumps. To begin, we can briefly drive the $S_{1/2} \leftrightarrow D_{5/2}$ transition with a 674-nm laser while the 422-nm light is blocked. After the laser pulse, we can ask whether or not the ion is in the long-lived ($\tau = 0.4$ s) $D_{5/2}$ state. To do this, we shine 422-nm and 1,092-nm light on the ion. If the ion is in the $D_{5/2}$ state, then neither of these lasers can drive a resonance in the ion; the detector that would observe 422-nm light from the atom *does not register any signal*. But if the 674-nm laser failed to drive the ion to the $D_{5/2}$ state, 422-nm and 1,092-nm light continually excites the atom, and the detector *registers tens of thousands of blue photons in a single second*. As we scan the 674-nm laser frequency, we observe a resonance such as that in Figure 4.

Instead of pulsing the red 674-nm laser light while the blue 422-nm laser light is blocked, we can leave all of the lasers on at the same time. Then it is as though the 422-nm light were continuously measuring whether or not the 674-nm laser has

Figure 2. (a) A rendering of the linear rf trap. Current traveling through the tungsten filament heats it to produce electrons, which are directed towards the trap by the bias grid. The strontium oven is heated so that the neutral atoms flow through the trapping region and collide with the electrons, making ions. To trap the ions, we apply potentials to the trap electrodes, $V_{rf} \sim 100$ to 200 V, $\Omega/2\pi \sim 7.1$ MHz and $U_0 \sim 50$ to 500 V. The trapped ions are immediately cooled to several mK by lasers propagating through the trap openings. In addition, the trap is placed in a vacuum chamber with pressure < 10^{-10} torr. The crystallized ions are depicted lying along the trap axis and (b) as imaged by our intensified CCD camera.

driven the atom into or out of the $D_{5/2}$ state. As quantum mechanics predicts, the results of such a measurement (i.e., is the atom in the $D_{5/2}$ state or not) should be unpredictable. Indeed, the 422-nm signal from the ion under these conditions is shown in Figure 5, and it randomly and suddenly switches between a large and small value. We collect such data in continuous blocks of approximately 30 minutes each, during which we monitor on the order of 10,000 quantum jumps. In total, we analyze 230,000 quantum jumps in a search for patterns or correlations in the times between jumps.[2]

Analyzing the Trapped-Ion Data

Although there are very many different statistical tests that have been performed on our data, we will illustrate only one in this article. We ask the following question: "If we are told the interval time between one set of quantum jumps, do we then have more information about subsequent interval times than we would otherwise?" The most direct way to answer this question is to measure the joint entropy between pairs of intervals. The entropy of a set of data tells us how many bits of data are required to describe the full data set; the more random the data, the higher the entropy. The joint entropy for two data sets tells us how many fewer bits are required to describe one data set if the other data set is known. We normalize this value so that if the data sets are completely correlated we obtain a value $U = 1$, and if they are completely unrelated, we obtain $U = 0$.

For example, if we have a stack of playing cards ordered by the face value of the cards (so the four 3s are together, the four 8s are together, etc.), if a 6 is drawn from the top of the deck then we immediately know that a 6 will be drawn from the top of the deck next. The normalized joint entropy, U, of pairs of cards drawn from this deck would be 1. If the deck of cards is shuffled well and we play this game long enough, we would find that the normalized joint entropy approaches zero.

Instead of using the values of playing cards, we use the interval times generated by the ion. Figure 6 represents a typical data set that we analyze this way. Here we have made a scatter plot of the lengths of adjacent intervals (T_i, T_{i+1}) during which the ion is scattering many blue photons (i.e., when it is not in the $D_{5/2}$ state). One feature we search for in such plots is asymmetry about the diagonal axis. For example, one possible result of potential memory in the ion (that is, nonrandomness) would be that a short interval, T_i, is more likely to be followed by a long interval, T_{i+1}, than a short interval. This would manifest itself by showing many more events in the upper left quadrant of the plot than in the lower right quadrant. We make such plots not only for consecutive intervals but also for intervals that are separated by up to 20 other intervals (i.e., we plot the frequencies of pairs $\{T_i, T_{i+k}\}$, where k ranges from 1 to 20). We also analyze intervals for which the ion is in the $D_{5/2}$ state and intervals between times of emitting a 674-nm photon and between times of absorbing a 674-nm photon. Qualitatively, we see no features in any of these graphs. Quantitatively, we calculate the normalized U between the two data sets comprising the first and second intervals for all the pairs of data. We find that $U < 7 \times 10^{-4}$ for all of our data and does not depend on the interval spacing for any of the different types of intervals. This analysis is an order of magnitude more sensitive than those previously performed on quantum jump data, and we expect to reduce our limit on U as we collect even more statistics.

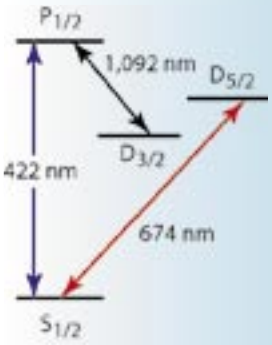
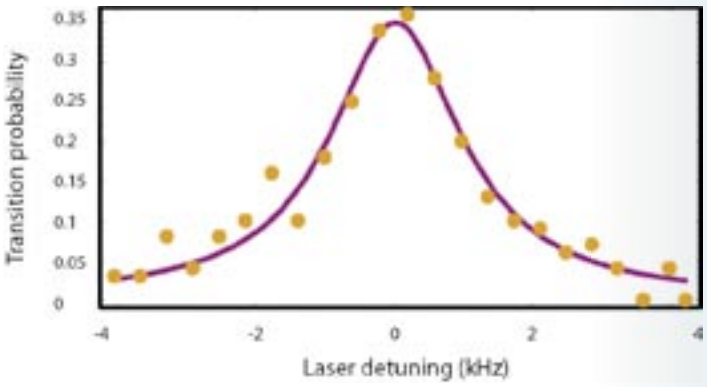


Figure 3. A partial energy level diagram of Sr^+. A frequency-doubled Ti:S laser drives the 422-nm transition to Doppler cool the ions, and we detect this scattered light to monitor the ions. A fiber laser drives the 1,092-nm transition to optically pump the ions out of the $D_{3/2}$ state. A diode laser with a bandwidth of < 2 kHz drives the 674-nm transition to induce quantum jumps and to coherently manipulate the ions.

Conclusion

Our experimental work has increased the sensitivity of our power to observe quantum effects and reduced the uncertainty in the randomness of those effects by over an order of magnitude. In addition to collecting more data with a recently improved laser system, we are developing the

Figure 4. Resonance curve of the $S_{1/2} \leftrightarrow D_{5/2}$ transition. At each frequency step, the 422-nm light is blocked and a 3-ms pulse of 674-nm laser light interacts with the ion. After each pulse, the state of the ion is measured by returning the 422-nm light to the ion. By repeating this process 100 times, we determine the average probability of exciting the ion from the $S_{1/2}$ to $D_{5/2}$ state. After accounting for broadening caused by laser intensity, we conclude that the laser linewidth is 1.3 kHz. This corresponds to jitter in the length of the 674-nm laser cavity of only 0.4 pm (the radius of a hydrogen atom in its ground state is 53 pm).



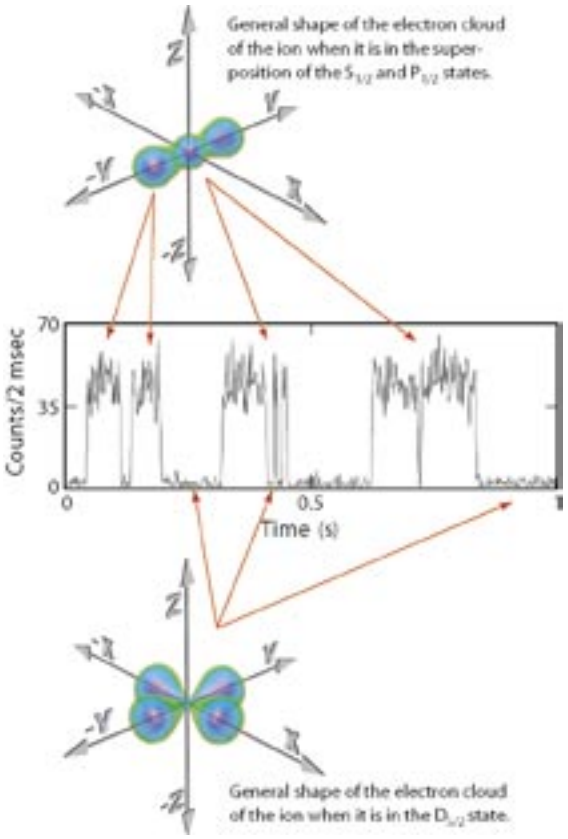


Figure 5. Quantum jumps in a single ion. Times at which the count rate is relatively high correspond to the atom being in a superposition of the $S_{1/2}$ and $P_{1/2}$ states. Times at which the count rate is very low are when the atom is in the $D_{5/2}$ state. Transitions between these two conditions indicate either the absorption or emission of a 674-nm photon.

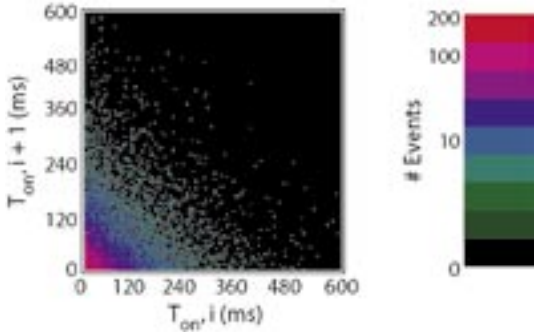


Figure 6. Scatter plot of the lengths of adjacent intervals during which the ion continually scattered 422-nm light.

capability to coherently control the external and internal states of the ion. We do this by driving the $S_{1/2} \leftrightarrow D_{5/2}$ transition with our narrow-bandwidth 674-nm laser, which can also cleanly couple specific quantized motional states of the trapped ion.

This work opens up the possibility of performing many other experiments. The ion can be laser-cooled to the ground state of its external motion where its temperature is nearly absolute zero. From this point, we can manipulate every physical aspect of the ion, tailoring its quantum-mechanical wavefunction as we see fit. We can control the interactions of the ion with the laser light to put it into quantum mechanical superpositions of states and observe their behavior and interactions with the environment. Or we can build a quantum logic gate for a quantum computer. And this, of course, is one of the motivations for testing the randomness of quantum mechanics as we have done.

References

1. D.J. Berkeland, "Linear Paul trap for strontium ions," *Review of Scientific Instruments* **73**(8), 2856–2860 (2002).
2. D.J. Berkeland, D.A. Raymondson, and V.M. Tassin, "Tests for non-randomness in quantum jumps," Los Alamos National Laboratory report (submitted 2003).

Acknowledgment

I am grateful for the efforts of Véronique Tassin and Daisy Raymondson (currently in the graduate program at the University of Colorado, Boulder) in the analysis and collection of statistics of transitions with multiple ions. This work was funded through the LANL LDRD program as part of 20020052DR, "Applied Quantum Technologies."

For further information, contact Dana Berkeland at 505-665-9148, djb@lanl.gov.

Atom Interferometry with Bose-Einstein Condensates

M.G. Boshier, C. MacCormick (P-21)

The demonstration in 1995 of gaseous Bose-Einstein condensation (BEC) took atomic physics into an exciting new regime in which the motion of large clouds of atoms is clearly governed by quantum, rather than classical, mechanics. All of the atoms in a condensate occupy the ground state of the potential well confining the system, so BEC represents the tightest control possible over matter. This control is at the heart of the field of coherent atom optics, in which the lenses, mirrors, and gratings of light optics are replaced by magnetic or optical potentials, which manipulate the atomic de Broglie wave. Figures 1 and 2 show two examples from our own laboratory of BEC atom optics.

As our next step in this area, we are developing techniques to divide a condensate into two (or more) coherent parts through appropriate manipulation of the confining potential. A division of the matter wave like this is analogous to a beamsplitter in optics. The analogy with optics can be carried further—the process of splitting the condensate (exposing one-half to a perturbation) and then recombining the two parts so that their wave functions can interfere forms an atom interferometer. These devices can respond with extreme sensitivity to any interaction that affects atomic energies. In addition, just as with light optics, the atom optical technology can also be miniaturized ultimately down to the level of an integrated "atom chip" with dimensions of just a few millimeters. Interferometry with BECs might therefore lead to a new generation of miniature sensors having unprecedented sensitivity to electromagnetic fields, to gravity and gravity gradients, and to accelerations. Focusing on just one of these interactions, sensitive instruments for measuring gravity have many important applications, such as underground structure detection; passive navigation and obstacle avoidance for submarines; and location of subterranean deposits of oil, minerals, and water.

Waveguide Interferometry

A simple calculation illustrates the power of atom interferometry—the earth's gravitational field causes the phase between two rubidium-atom wave packets separated vertically by 1 mm to evolve relative to each other at a rate of 2×10^6 cycles/s. It follows that an interferometer using a condensate of 10^6 atoms would have a statistical sensitivity to $\delta g/g$ of order 10^{-9} if the condensate was split for 1 s. This sensitivity is otherwise reached only by start-of-the-art laboratory instruments that are expensive, complicated, and most definitely not as portable.

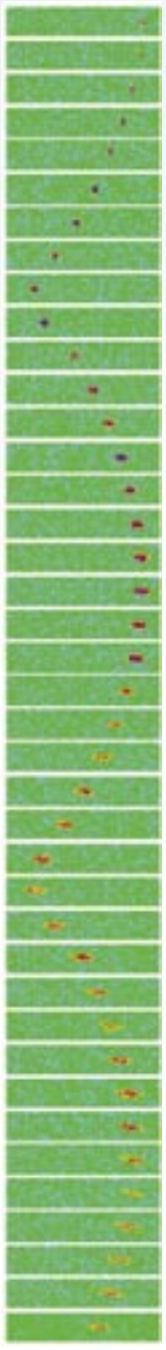


Figure 1. A BEC bouncing on a pulsed magnetic mirror.[1] The anisotropic expansion (fast in the vertical direction, slow in the horizontal direction) is a characteristic of the quantum evolution of the BEC. Images are 1.5 mm high and separated in time by 2 ms.

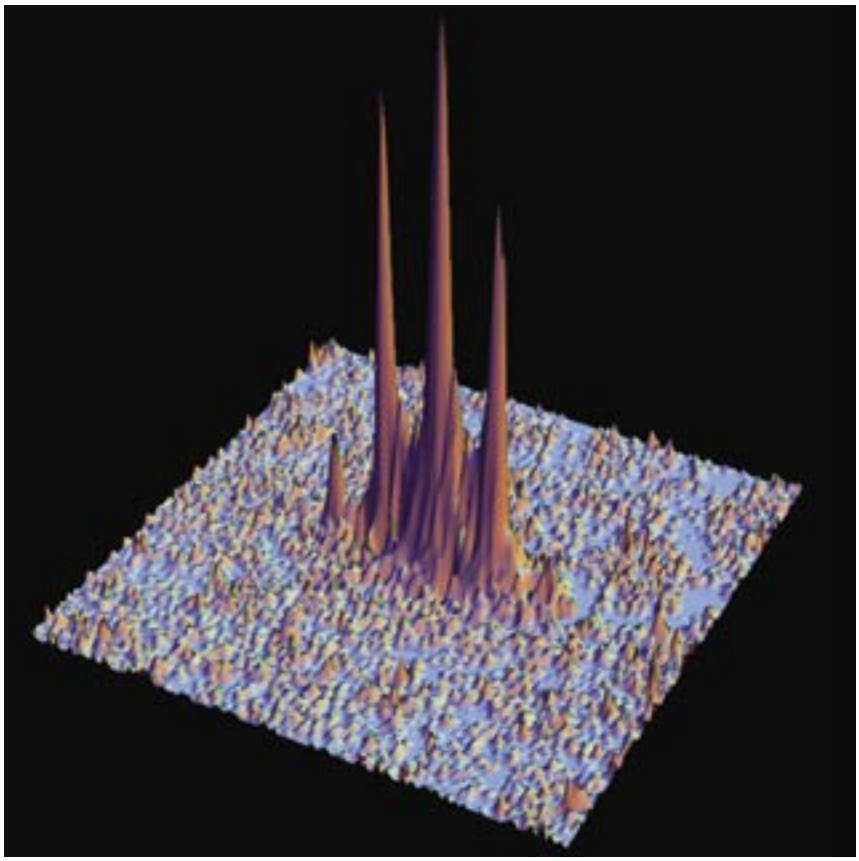


Figure 2. Diffraction of a BEC by a pulsed standing wave. The image shows the condensate density distribution after a free expansion that allows the momentum components created in the diffraction process to separate spatially.

The standing wave grating shown in Figure 2 can be used as the beamsplitter in a simple Mach-Zehnder-type interferometer (Figure 3), but the splitting time in this geometry is limited to much less than one second because the falling condensate soon hits the bottom of the apparatus. One can do considerably better by making use of the important fact that atoms, unlike photons, can be brought to rest, thereby allowing for very long measurement times. Because our stationary condensate interferometer design[1] has some similarities to light interferometers based on optical fibers, it is natural to refer to it as a condensate waveguide interferometer.

Implementation

Figure 4 illustrates the general principle of waveguide interferometry. The initial state is the condensate confined in the ground state of a thin, cylindrically symmetric harmonic waveguide potential. The potential is then deformed adiabatically into two separated waveguides (Step 1) forming a two-dimensional, double-well potential. In this process, the condensate wavefunction evolves into the symmetric ground state of this potential. Next (Step 2), the perturbation, V(t), under study is applied to one arm of the interferometer for time, τ, introducing a phase shift, ϕ, between the two arms. The resulting wavefunction can then be written in terms of the double-well eigenstates as a superposition of the degenerate symmetric and anti-symmetric ground states. The two arms of the interferometer are now overlapped by adiabatically transforming the potential back to the original single well. In this process (Step 3), the symmetric ground state of the double-well potential returns to the ground state of the single-well potential, and the anti-symmetric double-well state becomes the lowest-energy state of the single well with odd parity, i.e., the first excited state. The output ports of this interferometer in time are therefore the ground state and a first excited state of the waveguide. We present a full quantum-mechanical analysis of this interferometer in Reference 2. The process described above could also be realized as an interferometer in space using waveguides, which physically divide and recombine—in which case the device would resemble an optical fiber interferometer.

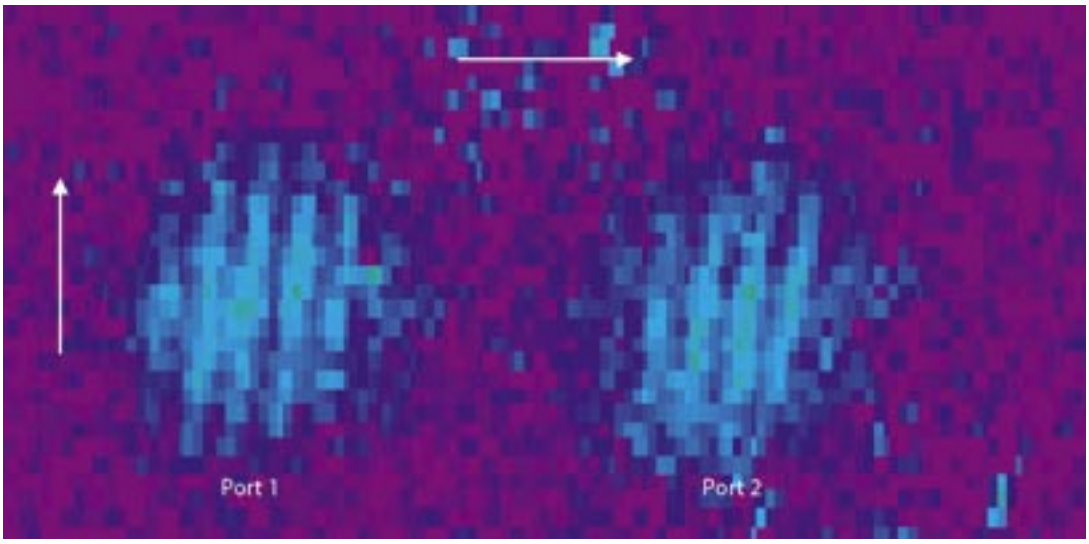


Figure 3. Interferometer fringes formed at the output ports of a freefall Mach-Zehnder condensate interferometer using standing-wave light pulses as beamsplitters.

We are exploring two complementary implementations of the waveguide interferometer—one based on magnetic forces and the other using the optical dipole force exerted by a far-detuned laser beam. The magnetic waveguide configuration consists of two long wires carrying currents in the same direction with a superimposed constant bias magnetic field applied parallel to the plane of the wires.[2] A waveguide for weak-field-seeking atoms (such as the F = 2, m = 2 ground-state atoms in our condensate) exists where the field is zero. We have shown that there are in general two such regions and that at a critical value of the bias field these two regions merge into a single waveguide. Increasing the bias field then splits the potential symmetrically into two, forming a beamsplitter. A full quantum mechanical analysis of this system can be found in our paper[2] along with a discussion of readout techniques—simple direct imaging of the condensate wavefunction is adequate, but there are better alternatives based on further manipulation of the potential.

The optical waveguide interferometer will make use of the optical dipole force, which pushes an atom towards a region of high intensity in a focused laser beam detuned below the atomic resonance. A low-power beam from an infrared diode laser can form a waveguide trap that confines a condensate for several seconds with negligible spontaneous emission. Radial trapping frequencies in such a trap are typically several kilohertz. This simple potential can be manipulated by scanning the laser beam through space at a much higher frequency (e.g., megahertz) than the trap frequency so that the condensate sees only the time-averaged potential. This promises to be a simple, yet powerful and flexible, approach to modifying the potential. A beamsplitter can be realized by passing the laser beam through an acousto-optic modulator used as a deflector to switch the beam back and forth between two positions whose separation increases

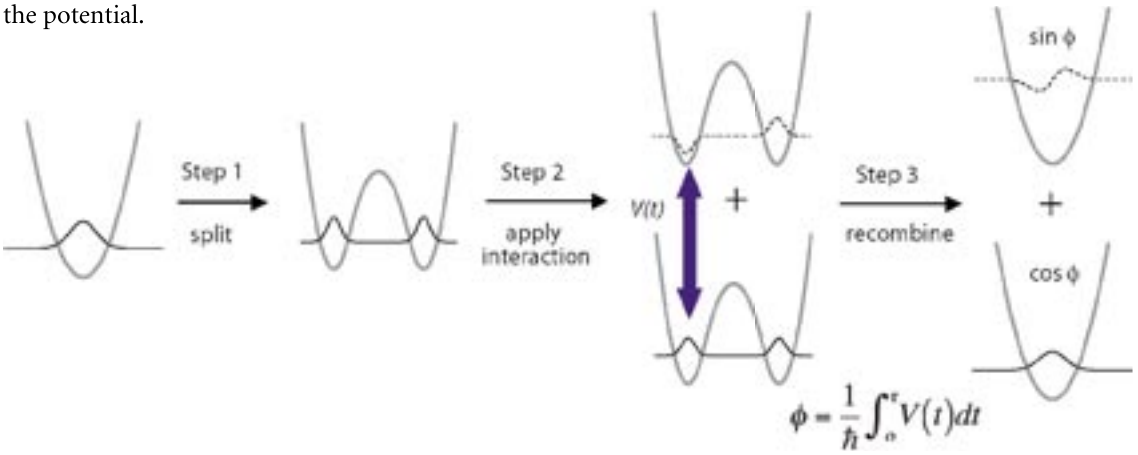


Figure 4. The waveguide interferometer.

slowly. The resulting time-averaged potential evolves into a double well. The scheme extends easily to more complicated geometries, such as dual interferometers for measuring gravity gradients, or to a potential that alternates between horizontal and vertical splitting to suppress systematic effects in a measurement of ***g***.

Conclusion

The sensitivity computed above is based on treating the condensate as a simple coherent matter wave in which each atom occupies the same single-particle state and interactions between atoms are negligible. Although this is the simplest regime in which to work initially, it should be possible to enhance the sensitivity by several orders of magnitude by harnessing the many-body nature of the condensate. The interactions between atoms in the condensate can be used to engineer exotic entangled states in which the measurement uncertainty scales with atom number N as 1/N, instead of the classical scaling factor $1/\sqrt{N}$. Not surprisingly, this enhanced sensitivity comes with a price, which in this case is a decrease in robustness to perturbations from the environment. The open problem of finding the optimal exotic states and devising techniques to create them in the laboratory is currently the subject of research by our T Division colleagues Diego Dalvit, Eddy Timmermans, and Daniel Steck.

References

1. A.S. Arnold, C. MacCormick, and M.G. Boshier, "An adaptive inelastic magnetic mirror for Bose-Einstein condensates," *Physical Review A* **65**, 031601(R), (2002).
2. E.A. Hinds, C.J. Vale, and M.G. Boshier, "Two-wire waveguide and interferometer for cold atoms," *Physical Review Letters* **86**, 1462, (2001).

Acknowledgment

Our work in this area is supported by funding from the LANL LDRD program.

For more information, contact Malcolm Boshier at 505-665-8892, boshier@lanl.gov.

Quantum Key Distribution

R.J. Hughes, J.E. Nordholt, C.G. Peterson, W.R. Scarlett, J. Anaya, D. Derkacs, J. Franken, P. Hiskett, W.J. Marshall, R. Sedillo, C. Wipf (P-21), K.P. McCabe, I. Bernstein, N. Dallman, I. Medina, P. Montano, N. Olivas, S. Storms, J. Thrasher, K. Tyagi, R.M. Whitaker (ISR-4), J. Wren (ISR-2), P. Milonni (T-DO), J.M. Ettinger, M. Neergaard (N-3), D. Ranken, R. Gurule (CCN-12)

On April 27, 1986, a satellite television broadcast to the east coast of the U.S. was briefly taken over by a hacker calling himself "Captain Midnight." With the growing reliance on satellites for communications, this notorious incident highlights the importance of assured command and control of orbital assets, as well as protection of downlinked data. In 1994, two LANL researchers, Richard Hughes and Jane Nordholt, set out a methodology whereby QKD using single-photon transmissions could be used to provide greater long-term security, based on fundamental principles of quantum physics, for secure satellite communications. Since then, our QKD team has been conducting research toward that goal, and we have developed another secure communications concept that would become possible with a satellite QKD capability—secure data dissemination between dynamically reconfigurable networks of users.[1] This research is leading to QKD becoming a higher-security alternative to present-day public-key-cryptography-based methods of establishing secure communication—today's public-key broadcasts, which we must assume are being recorded by adversaries, will become retroactively vulnerable if a large-scale quantum computer becomes feasible in the future, potentially allowing an adversary access to still-valuable information.

The Basics of Cryptography

The science of cryptography provides two parties ("Alice" and "Bob") with the ability to communicate with long-term *confidentiality*—they have the assurance that any third party (an eavesdropper, "Eve") will not be able to read their messages. Alice can encrypt a message ("plaintext"), P, before transmitting it to Bob, using a cryptographic algorithm, E, to produce a "ciphertext," C, which depends on K, a secret parameter known as a cryptographic key. [K is a random binary number sequence, typically a few hundred bits in length. For example, in the Advanced Encryption Standard the keys are up to 256 bits in length.] Bob is able to invert the encryption process to recover the original message, P, provided he too knows the secret key, K. Although the encryption algorithm E may be publicly known, Eve passively monitoring transmission C would be unable to discern the underlying message, P, because of the randomization introduced by the encryption process—provided the cryptographic key, K, remains secret. (The algorithm E is designed so that without knowledge of K, Eve's best strategy is no better than an exhaustive search over all possible keys—a computationally infeasible task.) In this so-called *symmetric key* cryptography, *secret* key material is therefore a very valuable resource, but there is an underlying problem; before Alice and Bob can communicate securely it is of paramount importance that they have a method of securely distributing their keys. It is this problem of key distribution that QKD solves, providing the ultimate security assurance of the laws of physics (Figure 1).

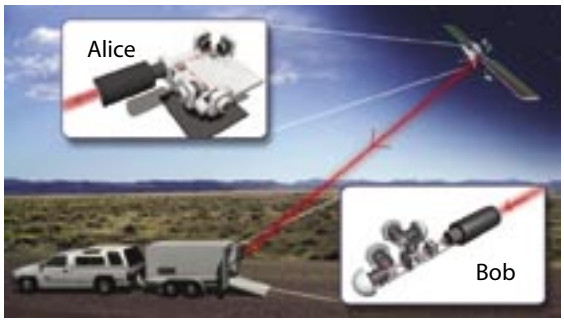


Figure 1. In our conceptual satellite QKD system, the transmitter of the quantum key material (Alice) is on the orbiting satellite and the receiver (Bob) is on the ground. Alice's four attenuated lasers (top left) will transmit polarized photons to Bob's receiving telescope (lower right), which collects them and directs them to one of four detectors. The registered signal from these detectors forms the raw key material for a cryptographic system whose secrecy is guaranteed by the laws of quantum physics.

The QKD Concept

QKD was first proposed in 1984 by Charles Bennett (IBM) and Gilles Brassard (University of Montreal). Alice and Bob, equipped with the ability to perform conventional, nonsecret ("public") but authenticated communications with each other, could produce copious quantities of shared, secret random key bits, for use as cryptographic keys, by using quantum communications. In their "BB84" QKD protocol, Alice (the transmitter) sends a sequence of random bits over a "quantum channel" to Bob (the receiver) that are randomly encoded as linearly polarized single photons in either of two conjugate polarization bases with (0, 1) = (H, V), where "H" ("V") denotes horizontal (vertical) polarization (respectively), in the "rectilinear" basis, or (0, 1) = (+45°, -45°), where "+45°" and "-45°" denote the polarization directions in the "diagonal" basis. Bob randomly analyzes the polarization of arriving photons in either the rectilinear or diagonal basis, assigning the corresponding bit value to detected photons. Then using the public channel, which is assumed to be susceptible to passive monitoring by Eve, he informs Alice in which time slots he detected photons but without revealing the bit value he assigned to each one.

Next, Alice reveals her basis choice for each bit but not the bit value. Bob communicates back the time slots of his detected bits for which he used the same basis as Alice. In an ideal system, Alice's transmitted bits and the results of Bob's measurements on this random, matching-basis portion, known as the "sifted" key, are perfectly correlated; they discard the bits for which Bob used the wrong basis (e.g., his receiver "looked" in the diagonal basis when she transmitted the bits in the rectilinear basis and *vice versa*) (Figure 2).

In practice, Bob's sifted key contains errors. Fundamental quantum principles ensure that Eve is both limited in how much information she may obtain by eavesdropping on the quantum communications and that she cannot do so without introducing errors in Bob's sifted key from which Alice and Bob can deduce a rigorous upper bound on leaked information. Alice and Bob determine this bound after reconciling their sifted keys using *post facto* error correction over their public channel. From their partially secret reconciled keys, Alice and Bob extract the shorter, final *secret* key after a final stage known as "privacy amplification." For example, if Alice and Bob form the parities of suitable random subsets of their reconciled bits, they can be sure that Eve will be ignorant of at least one of the bits in each subset and hence ignorant of the final secret bits.

Free-Space QKD

A satellite-to-ground free-space QKD capability has particularly appealing security features. Typically, satellites are launched with all the keys they will ever have but they may exceed their design lifetime or they may need to encrypt more data than expected. Then one must face the challenge of providing new keys to a possibly very high-value satellite asset on-orbit. Clearly it is infeasible to use a human courier for this task, and although public-key cryptography allows keys to be transferred conveniently, its use already presents a latent vulnerability to unanticipated computation advances, including quantum computers. In contrast, QKD provides much greater long-term security guarantees—it can only be attacked by technology in existence at the time of transmission and cannot be attacked by a quantum computer. A second advantage of QKD is in the context of *key generation*; it allows a fresh key to be produced at transmission time using the intrinsic randomness of quantum mechanics. This could be very useful to support the demands for large amounts of key material within a transformational communications scenario, as well as reducing the risks associated with conventional keys—that they might be (accidentally or maliciously) compromised by insiders. Finally, QKD narrows an adversary's window of opportunity; Eve's best strategy is to attempt a "man-in-the-middle" attack, but to do so she would have to break the initial authentication

in time to insert herself into the channel between Alice and Bob. Breaking the authentication *after* the quantum communications have taken place is of no use to Eve.

For satellite-to-ground (or any other line-of-sight application) QKD, one must reliably transmit and detect single photons through the atmosphere in the presence of background radiance, which is a strong error source even at night. We effectively deal with this challenging problem using a combination of spectral, spatial, and temporal filtering. The synchronization requirements are especially important; we must only accept photons that reach the receiver within specific 1-ns time windows. Our solution to this difficult problem makes QKD possible even in full daylight, which is one of the unique features of our research that sets us apart from our competitors.

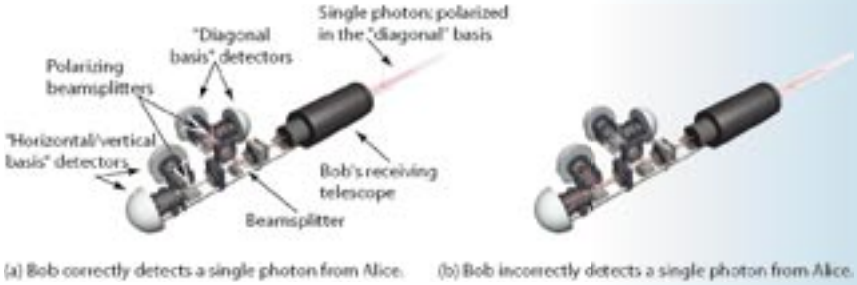
In 2001, using a readily transportable system, we carried out a QKD experiment over a 10-km line-of-sight range between Pajarito Mountain and TA-53, LANL, which had optics (extinction of one air mass, background, and turbulence) representative of a satellite-to-ground path.[2] We were able to reliably produce shared, secret keys at rates of several hundred bits per second throughout the day and night (i.e., 1–2 keys per second). On each clock cycle (1 MHz at the time), the transmitter (Alice) generates two secret random bits, which determine which one of four attenuated "data" diode lasers emits about a 1-ns optical pulse with one of the BB84 polarizations (see the Alice inset in Figure 1) and an average photon number less than one (with Poissonian photon-number statistics) that is launched towards the receiver (Bob). At Bob, a telescope collects the data pulse and directs it into an optical system where its polarization is randomly analyzed in one of the BB84 bases. Single-photon detectors, one for each of the four BB84 polarizations, register the result (see the Bob inset in Figure 1). This process is repeated for one second, following which the session is completed with the various public-channel processes (sifting, reconciliation, and privacy amplification) using a wireless Ethernet connection before starting up the next 1-s session. (In subsequent work using the data from this experiment, we implemented for the first time in QKD research the all-important authentication aspect and demonstrated that self-sustaining, authenticated, secret-key production is possible with minimal overhead in secret bits.) The background rejection in our system was sufficiently high that we were even able to transfer secret key bits under worst-case conditions with the sun directly illuminating the receiver.

Implications and Developments for Satellite QKD

With input from the results of this experiment, we have developed a model that allows free-space QKD performance to be predicted in other regimes. In particular, we have modeled a QKD link between a satellite and a ground location.[3] We have determined that it is optimal to locate the transmitter (Alice) on the satellite and the receiver (Bob) on the ground so that the optical effects of atmospheric turbulence are in the transmitter's far-field zone. For low-earth-orbit (LEO) satellites, we find that useful QKD contacts can be established over wide areas of the earth's surface, day or night, using only modest-scale (~ 50-cm in diameter) optical ground facilities, whereas with larger aperture (> 1-m in diameter) optical ground facilities, QKD from higher altitude orbits (such as geosynchronous ones) would be feasible at night.

We have also developed a preflight QKD transmitter (a so-called "brassboard"). This device is sufficiently small and lightweight that it could be accommodated on a satellite, yet sufficiently rugged that it could survive the rigors of launch. So far, we have tested this in a laboratory environment and produced large quantities of high-quality, secret key

Figure 2. The raw QKD key material must be "sifted" to produce useful, matching bit strings. In this example, Bob is receiving a single photon that Alice transmitted in the "diagonal" basis (see text for details). The first beamsplitter randomly directs the photon either to the right (a) or straight ahead (b). If the photon goes to the right, a second polarizing beamsplitter will direct it to the correct "diagonal basis" detector, and it becomes a useful bit of key material (a "1" or a "0"). If the photon goes straight ahead, another polarizing beamsplitter will randomly send it to a "horizontal/vertical basis" detector—this randomness eliminates its usefulness as key material. Bob communicates with Alice over a public channel how he detected each photon—but not the result. Alice tells Bob which photons were tested correctly, and those bits form the "sifted" cryptographic key.



bits. The performance of this device, together with our modeling results give us great confidence that satellite-to-ground QKD would be possible at useful rates with existing technology.

It is likely that on-orbit re-keying would be performed with a QKD ground unit located at a satellite's operations center or mission-control center, but the modest parameters required of a ground-receive unit (for LEO satellites) suggests another use—the transfer of keys between ground users via a QKD-capable satellite. For example, a QKD capable satellite could generate keys with each of two QKD ground units in different parts of the world (which could be transportable systems). The satellite could then communicate to the second user which bits to flip so that his key matches the first user's; this information could be sent in the clear without compromising security. These ground users could now establish secure communications over any convenient channel using this shared key. Several cross-linked QKD-capable satellites could support worldwide on-demand secure communications to the coalitions of land-, sea-, air-, and space-based users envisioned in emerging "transformational-communications" concepts. This concept can be further extended with optical-fiber QKD links to the satellite QKD ground units. Building on previous work in which we have demonstrated QKD over a 48-km optical-fiber path in LANL's network,[4] we have recently shown the feasibility of the much harder problem of performing QKD over a fiber that is also carrying network traffic.[5] Optical-fiber QKD would therefore not require a dedicated fiber connection.

Conclusion

While considerable basic and applied research remains to be done, QKD is the first aspect of quantum information science to enter the technology-development era; it is possible with existing technology and is capable of providing solutions to the pressing secure-communications requirements of the next decade. The LANL QKD team is in the forefront of this "first wave" of QKD research and development, but we are also engaged in the basic research of the "second wave" of QKD that will be based on the uniquely quantum-mechanical properties of "entangled" two-photon states.

References

1. R.J. Hughes and J.E. Nordholt, "A new face for cryptography," *Los Alamos Science* **27**, 68–85 (2002).
2. R.J. Hughes, J.E. Nordholt, D. Derkacs *et al.*, "Practical free-space quantum key distribution over 10 km in daylight and at night," *New Journal of Physics* **4**, 43.1–43.14 (2002).
3. J.E. Nordholt, R.J. Hughes, G.L. Morgan *et al.*, "Present and future free-space quantum key distribution," in *Free-Space Laser Communication Technologies XIV*, G.S. Mecherle, Ed. (SPIE, Bellingham, Washington, 2002), Proceedings of SPIE Vol. 4635, pp. 116–126.
4. R.J. Hughes, G.L. Morgan, and C.G. Peterson, "Quantum key distribution over a 48-km optical fiber network," *Journal of Modern Optics* **47**, 533–547 (2000).
5. P. Tolliver, R.J. Runser, T.E. Chapuran *et al.*, "Experimental investigation of quantum key distribution through transparent optical switch elements," *IEEE Photonics Technology Letters* **15**(11), 1669–1671 (2003).

Acknowledgment

It is a pleasure to acknowledge collaborations with P. Kwiat of the University of Illinois; S. Nam, A. Miller, and D. Rosenberg of the NIST; A. Ellsasser, M. Dulski, R. Baker, and R. Trevino of the DoD; R. Blake, S. McNown, P. Hendrickson, R. Shea, and T. Persons of the U.S. government; M. Goodman, R. Runser, T. Chapuran, P. Tolliver, and J. Jackel of Telcordia; and N.C. Donnangelo of The MITRE Corporation. This research was funded by the Advanced Research and Development Activity and the Secretary of the Air Force.

For further information, contact Richard Hughes at 505-667-3876, hughes@lanl.gov, or Jane Nordholt at 505-667-3897, jnordholt@lanl.gov.